



RISK ADVISORY SERVICES

Critical Infrastructure Bill – Risk Management

We are seeing major breaches or incidents practically every week at a global or national scale impacting organisations of all sizes. As the threat landscape changes and cyber security morphs into cyber warfare, organisations within a given nation are becoming collateral damage as nation states fight for supremacy in the cyber world as well as areas of innovation, and research and development.

Having recognised this, the Australian Federal Government has taken the step to boost protection with better risk management for organisations deemed to be critical infrastructure by introducing the Critical Infrastructure Bill. The Critical Infrastructure Bill better defines what critical infrastructure is, expands the sectors that are now considered critical infrastructure and introduces a principles-based outcomes approach to risk management covering the following key risks:

- Physical
- Cyber
- Personnel
- Supply chain

There are eleven critical infrastructure sectors:

- Communications
- Data Storage or Processing
- Defence Industry
- Financial Services and Markets
- Food and Grocery
- Higher Education and Research
- Health Care and Medical Sector
- Transport
- Energy
- Space Technology
- Water and Sewerage

Benefits of a Critical Infrastructure Bill – Risk Management

The *Critical Infrastructure Bill – Risk Management* introduces new requirements intended to uplift core security practices of critical infrastructure assets by ensuring responsible entities take a holistic and proactive approach toward identifying, preventing and mitigating risks from all hazards. The Bill sets out the overarching obligations, whilst more detailed sector-specific requirements will be contained in rules.

The view of the Department of Home Affairs is that good risk management practice entails both identifying and mitigating material risks that may have a significant relevant impact on their critical infrastructure assets. Requiring entities to demonstrate that they are thinking about risk management holistically in their business helps to ensure that risk processes are robust.

A complete approach to risk management

Our *Critical Infrastructure Bill – Risk Management* offering is a simple and effective approach to understanding and managing key risks around the four risk areas as defined by the Critical Infrastructure Bill. Organisations will need to continue to focus on the core activities they perform. RSM's comprehensive risk management offering will cover all four risk areas as you continue your core activities delivering the following principles-based outcomes, in the design and development of an effective critical infrastructure risk management program:



- Identification of material risks
- Mitigation of risks to prevent incidents
- Minimise the impact of realised incidents
- Effective governance

We assist by supporting organisations in the development of a comprehensive understanding of the threat picture that can affect the availability, confidentiality, reliability and integrity of the relevant critical infrastructure asset. There is no one-size fits all approach.

Benefits of a Critical Infrastructure Bill – Risk Management Engagement

- Identification of potentially critical risks and issues
- Establishment of a baseline for risk management at your organisation
- Monetary quantification of cyber risk exposure to assist in cyber risk remediation activities
- Provides critical cyber risk quantification information for cyber risk insurance policy cover



Who needs a Critical Infrastructure Bill – Risk Management?

A Critical Infrastructure Bill – Risk Management offering can help your organisation if you need a better understanding of your risk exposure for the four key risk areas defined in the Critical Infrastructure Bill. The assessment is also useful in communicating risk management maturity and cyber risk exposure value to key stakeholders.

What we deliver

As part of the Critical Infrastructure Bill – Risk Management offering, we deliver four assessment reports against each of the four key risk areas that includes the following key components:

- **Conclusion** – outlining your risk management maturity and risk exposure
- **Impacts** – an outline of material risks and impact on the business of an incident
- **Guidance** – on remediation effort going forward allowing you to minimise the impact of an incident as well as establishing an effective governance framework

For more information please contact:

Ashwin Pal

Partner, Sydney
T 02 8226 4500
E ashwin.pal@rsm.com.au

Darren Booth

Partner, Melbourne
T 03 9286 8158
E darren.booth@rsm.com.au

Jacob Elkhishin

Partner, Brisbane
T 07 3225 7819
E jacob.elkhishin@rsm.com.au